Big Brother's Geschäftspartner: Privatheit und Überwachung in den USA nach dem 11. September 2001

Rürup, Katharina Sophie

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Katharina Sophie Rürup (Berlin)

Big Brother's Geschäftspartner:
Privatheit und Überwachung in den USA nach dem 11. September 2001

*Im Gefolge der Anschläge vom 11. September 2001 zeichnen sich neue Gefährdungen von Privatheit in den USA ab. Um diese besser zu begreifen wird der (rechtshistorische) Hintergrund amerikanischer Konzepte von „*Privacy*" (Privatheit, Privatsphäre) erläutert. Zu diesem Zweck rekonstruiert der Artikel zunächst Konzepte von* Privacy *in der amerikanischen Verfassungsrechtsprechung und skizziert die vorhandene amerikanische* Privacy*-Gesetzgebung. Im Anschluss werden die rechtlichen Entwicklungen nach dem 11. September (vor allem im* USA PATRIOT Act*) geschildert und dabei der Themenkomplex der Datenüberwachung und –auswertung herausgegriffen, um die Auswirkungen auf den Schutz der Privatsphäre sowie die Schwierigkeiten, die sich aus der spezifisch amerikanischen rechtlichen Tradition in diesem Bereich ergeben, zu erläutern. Abschließend werden verschiedene Ansätze diskutiert, mit der neuen Qualität von Datenüberwachung in den USA umzugehen und die Möglichkeit eines positiven Rechtes auf Privatheit besprochen.*

Keywords: US-amerikanische Innenpolitik, Supreme Court, Privatheit, Sicherheitsgesetze, Vierter Verfassungszusatz, Datenschutz
American domestic policy, Supreme Court, privacy, Patriot Act, Fourth Amendment, data mining

1. Einleitung

Nach dem 11. September 2001 hat die US-Regierung eine Anzahl von Initiativen ergriffen, die einen verstärkten Eingriff in die Privatsphäre des/der Einzelnen darstellen: Zugriff auf bisher private Daten ohne richterlichen Beschluss, Ausweitung der Überwachung von Telephongesprächen und Emailverkehr, Abhören von Anwalt-Klientengesprächen, gesteigerte Überwachung von TouristInnen und ImmigrantInnen und routinemäßige Untersuchung von Personen und Gepäckstücken an Flughäfen, Bahnhöfen und beim Eintritt in öffentliche Gebäude. Robert Pitofsky, Leiter der *Federal Trade Commission* unter Clinton und eigentlich bekannt für seine positive Einstellung zum Datenschutz, meinte nach den Anschlägen: „September 11 changed things. Terrorists swim in a society in which their privacy is protected. If some invasions of privacy are necessary to bring them out into the open, most people are going to say, ‚O.K., go ahead'" (zit. nach France/Green 2001). All diese neuen Entwicklungen haben bei BeobachterInnen Sorgen aufkommen lassen, ob sich die USA auf dem Weg in den Überwachungsstaat befinden und damit den schützenden „Raum" des Privaten einengen oder gar aufheben. Diese Sorgen haben im Zuge des amerikanischen Zugriffs auf Passagierdaten im Flugverkehr oder andere Formen des transnationalen Datentransfers inzwischen auch Europa erreicht (Regan 2003).

Sorgen um das „Ende der Privatsphäre" sind nicht neu – wer erinnert sich nicht an die ubiquitären Warnungen vor „1984" im Zuge der Volkszählungsdebatte in der BRD in den 1970er und 1980er Jahren. Nachdem dann der erwartete Schrecken eine Weile ausblieb, geriet George Orwell ein wenig in Vergessenheit: Eine

Zeit lang schien es, als sei nicht mehr der Überwachungsstaat als zentral hierarchisches Gebilde die Gefahr, sondern ein Konglomerat aus privatwirtschaftlichen Überwachungsaktivitäten am Arbeitsplatz und in den nicht mehr öffentlichen Räumen von Freizeit und Konsum. Mit dem 11. September und den seither in den USA und anderen Staaten eingeleiteten Veränderungen in der Strafverfolgung und Ermittlung ist die Überwachungstätigkeit des Staates ins Zentrum des öffentlichen Interesses an der Überwachung zurückgekehrt.

Im Unterschied zu der Situation vor 25 Jahren scheint es kaum noch technische Grenzen der Überwachungsmöglichkeiten zu geben. Die Diskussion muss heute davon ausgehen, dass der Staat und der private Sektor noch nie da gewesene Möglichkeiten haben, persönliche Daten zu sammeln, und dass die technische Entwicklung zu einem Sinken der Überwachungskosten und einem weiteren Anwachsen der Datenmassen führen wird. Durch technische Entwicklung, Globalisierung, also Datenfluss über Grenzen hinweg, Konvergenz der Technologien, also Integration der Systeme, und durch Multimedia, d.h. die Verbindung vieler Übertragungs- und Darstellungsformen, wodurch eine Informationsart leichter in eine andere überführt werden kann, können diese Datenmengen jetzt – theoretisch – in großen Datenbanken gemeinsam verwaltet und ausgewertet werden.

Der Schwerpunkt dieses Artikels liegt nicht auf der Gewinnung von Daten, sondern auf deren Kollationierung, d.h. auf ihrer Zusammenführung und Auswertung. Ich werde – davon ausgehend, dass alle gewonnenen Informationen digitalisiert und in Datenbanken gespeichert werden – mich mit dem beschäftigen, was in der amerikanischen Diskussion als *data mining*, als *datasurveillance* oder manchmal auch schon als *dataveillance* (Clarke 1988) bezeichnet wird und dabei diskutieren, inwieweit durch das Kollationieren von Daten eine neue Qualität entsteht, die auch einen neuen Ansatz in der rechtlichen Behandlung von Privatheit erfordert.

Auch wenn diese Entwicklung – besonders im privatwirtschaftlichen Bereich – nicht neu ist, gewinnt sie doch nach dem 11. September neue Qualitäten. Diese werde ich versuchen zu verdeutlichen, in dem ich a) das Sicherheitspaket, das in den USA nach dem 11. September verabschiedet wurde (den *PATRIOT Act*) und die dadurch erweiterten Überwachungsmöglichkeiten skizziere und b) die verschiedenen, seither aufgelegten *data mining*-Programme der amerikanischen Regierung (TIA und MATRIX) darstelle. Die Problematik dieser Programme und die Kritik, die Bürgerrechtsorganisationen daran geäußert haben, machen die Schwierigkeiten deutlich, auf diesem Feld mit dem bestehenden Instrumentarium der amerikanischen Privatheitsrechtsprechung auszukommen.

In Anbetracht der technischen Entwicklung wird mehr denn jemals zuvor Überwachung nur noch durch rechtliche Bestimmungen limitiert. Aus diesem Grunde scheint es sinnvoll, sich mit der Konstruktion von Privatheit im politischen und rechtlichen Diskurs in den USA zu beschäftigen. Um den Hintergrund der amerikanischen Positionen zu erhellen, ist es nötig, *Privacy* (Privatheit) sowohl als allgemeines Konzept als auch schützenswertes Rechtsgut in der Tradition der amerikanischen Rechtsprechung zu betrachten.[1] Es werden hier daher zunächst die theoretischen, verfassungsrechtlichen und im *Common Law* wurzelnden Ursprünge der amerikanischen Auffassung von Privatheit dargestellt. Darauf folgend werden die zentralen Urteile des *Supreme Court* geschildert und wie sich in ihnen die jeweilige zeitgenössische Auffassung von Privatheit spiegelt. Zu berücksichtigen ist hier, dass die amerikanische Verfassungsrechtsprechung unterschiedliche Formen von Privatheit kennt. Ich werde mich hier auf die informationelle Privatheit beschränken und möchte die anderen nur erwähnen, um den Kontext der Debatten zu verdeutlichen.

Der amerikanische Ansatz in Sachen Schutz der Privatsphäre und Datenschutz ist es, spezifische und sehr begrenzte Gesetze zu schaffen, die auf Daten in einem jeweiligen konkreten Kontext abgestellt sind. Er zielt dabei zu weiten Teilen lediglich auf staatlicherseits erhobene und gesammelte Daten, im Gegensatz zur europäischen Praxis der übergreifenden Idee der

informationellen Selbstbestimmung, die in Artikel 8 der europäischen Grundrechtscharta, dem Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten von 1981 und in den EU-Datenschutzrichtlinien von 1995 verankert ist (Stratford/Stratford 1998).

Neben dem Schutz der informationellen Freiheit kennt die US-Rechtsprechung eine Privatheit nach dem ersten Verfassungszusatz, denn zum Recht auf freie Meinungsäußerung gehören auch das Recht, Meinungen anderer nicht zur Kenntnis zu nehmen sowie das Recht anonym zu bleiben (Brenner 2002,137ff.).[2] Zusätzlich kennt das amerikanische Recht die dezisionale Privatheit (Rössler 2001, 170ff.). Diese wurde seit 1973 in der Entscheidung des *Supreme Court* zur Abtreibungsfrage in *Roe v. Wade* ausgeformt und gründet auf dem Recht des/der Einzelnen, grundsätzliche Lebensentscheidungen ohne staatliche Bevormundung treffen zu können. Welche Entscheidungen für den/die Einzelne/n so zentral sind, dass sie in seine/ihre Persönlichkeitsrechte eingreifen, ist nicht abschließend geklärt. Aber eine Vielzahl von Entwicklungen – vor allem im biotechnischen und medizinischen Bereich – verlangt zunehmend mehr Entscheidungen des/der Einzelnen, die tiefgreifende Auswirkungen auf sein/ihr Leben haben und daher nach der Logik von Roe nicht staatlichen Eingriffen unterliegen dürfen, sondern im Ermessen des/der Einzelnen liegen. Deswegen lag vor dem 11. September die Vermutung nahe, dass in der Rechtsprechung des *Supreme Court* zukünftig Fragen der dezisionalen Privatheit eine weitaus größere Rolle spielen würden als Fragen der informationellen. Nach den politischen Ereignissen der letzten Jahre steht aber nun genau die gegenteilige Entwicklung ins Haus: Die informationelle *Privacy* scheint das zentrale Anliegen der nächsten Jahre zu sein.

2. *Privacy* in der amerikanischen Rechtstradition

Was aber ist denn so schlimm an staatlicher Datensammlung und Überwachung? Zumal wenn wir einmal davon ausgehen, dass es sich um Überwachung und Datensammlung durch eine demokratisch gewählte Regierung handelt? Liegt es denn nicht eigentlich im Interesse der BürgerInnen, dass der Staat eine seiner primären Funktionen, nämlich ihr Leben und ihre Gesundheit zu schützen, wahrnimmt? Und kann er dies nicht umso besser, je mehr Informationen ihm hierbei zur Verfügung stehen?

Danach zu fragen, warum unterschiedliche Formen der Beobachtung und der Übermittlung von Daten problematisch sind und warum sie als gefährlich betrachtet werden können, heißt danach zu fragen: Warum schätzen wir die Privatsphäre, warum ist Privatheit wertvoll? Und vor allem, was eigentlich verstehen wir unter „Privatheit"? Es gibt eine Unzahl von Versuchen, diese Frage zu beantworten und einen normativen Begriff von Privatheit zu entwickeln. Viele der Antworten drehen sich um Privatheit als Voraussetzung für oder Ausdruck von Persönlichkeit, oder sie begreifen Privatheit als Freiheit des autonomen Individuums, seinen eigenen Gedanken, Handlungen und Entscheidungen nachzugehen (Rössler 2001).[3] Eine dritte Variante, in den USA vor allem von Alan F. Westin vertreten, ist die Vorstellung von Privatheit als Kontrolle über Informationen: „Privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others" (Westin 1967, 7) – was häufig als informationelle Privatheit bezeichnet wird. Grundidee der informationellen Privatheit ist, dass sie einen Schutz gegen Beobachtung durch Voyeure, durch Kameras im öffentlichen Raum oder durch Datensammler, kurz: durch bestimmte oder unbestimmte Dritte darstellt – wobei die Frage, was genau geschützt werden soll, umstritten ist.

Die Schwierigkeiten der theoretischen Definition von Privatheit reflektieren nicht nur kulturelle Unterschiede zwischen „europäisch-kontinentalen" und angelsächsischen Traditionen, sondern zunächst die Vielfältigkeit des juristischen und politischen Sprachgebrauchs. Es gibt in der amerikanischen Verfassung kein explizites Grundrecht auf Privatheit. Es handelt sich in allen Fällen um ein abgeleitetes Recht

und dessen konkrete Ausformung in den letzten 100 Jahren, meistenteils durch die Rechtsprechung des obersten Verfassungsgerichts.[4] Es werden daher im Folgenden in der Hauptsache Urteile des *Supreme Court* herangezogen, um die Frage zu beantworten, wie sich die Rechtsauffassung von Privatheit in den letzten 100 Jahren in den USA entwickelt hat, welche sozialen (und technischen) Entwicklungen die Vorstellungen von Privatheit verändert haben und welche Veränderungen notwendig sind, um auf neuartige Bedrohungen der Privatsphäre reagieren zu können.

Auch wenn der Schutz der Privatsphäre in den USA zunächst nicht explizit formuliert wurde, enthält natürlich bereits die *Bill of Rights* eine Reihe von Passagen, die das Privateigentum, besonders das Privathaus, vor staatlichem Zugriff schützen. Z.B. erklärt das *Third Amendment* Einquartierungen von Soldaten in Privathäusern ohne Einwilligung des/der Eigentümers/Eigentümerin ausdrücklich für unzulässig, und das *Fourth Amendment* setzt klare Grenzen für Durchsuchungen und Beschlagnahmungen:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized (zit. nach Stanley/Steinhardt 2003, 16).

Seine Wurzeln hat dies in der englischen Rechtstradition des „*my home is my castle*". Auch Konzepte von „unbefugtem Betreten" von privatem Grund und Boden durch Mensch oder Vieh gibt es bereits in der frühen amerikanischen Rechtstradition. Privatheit ist also kein neues Konzept, sondern wurzelt in modernen Begriffen von persönlicher Freiheit und Eigentum, wird jedoch nicht explizit erwähnt, weder in Gesetzestexten noch in Urteilen oder Kommentaren.

Die Tradition von Privatheit (*Privacy*) als Rechtsbegriff in den USA beginnt 1890 mit Samuel Warrens und Louis Brandeis' Aufsatz „*The Right to Privacy*" in der *Harvard Law Review*. Sie leiteten ein Recht auf Privatheit aus der *Common Law*-Auffassung ab, dass jedes Individuum ein Recht darauf habe zu entscheiden, „to what extent his thoughts, sentiments, and emotions shall be communicated to others" (Warren/Brandeis 1890, 198), und stellten fest, dass es bisher nur die Möglichkeit gäbe, gegen Veröffentlichungen rechtlich vorzugehen, wenn es sich um Verleumdung oder üble Nachrede handle, nicht aber gegen die Tatsache der Veröffentlichung als solche. Ihnen aber ginge es nicht um den Wahrheitsgehalt, sondern um das Recht auf Privatheit, das sie als „right to be let alone" (Warren/Brandeis 1890, 195) definierten. Besonders hervorzuheben ist hier, dass Warren und Brandeis ihren Ausgangspunkt und ihre Argumentation aus der Entwicklung neuer – Privatheit gefährdender – Technologien („recent inventions and business methods") ableiteten.

> Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that ‚what is whispered in the closet shall be proclaimed from the house-tops' (Warren/Brandeis 1890, 193).

Privatheit als *legal term* steht also von Anbeginn an in einem engen Zusammenhang mit gesellschaftlichen und technischen Entwicklungen wie Industrialisierung, Urbanisierung und der Entwicklung von Massenmedien. In diesem frühen Text wird Privatheit tatsächlich nicht als liberales Abwehrrecht gefasst, eine Auffassung, die aber dann – wie wir im Folgenden sehen werden – so in der Rechtstradition der USA keine Fortsetzung gefunden hat.[5]

Noch 1928 stellte der *Supreme Court* in *Olmstead v. United States* fest, das Abhören von Telefongesprächen stelle keine Verletzung des Vierten Verfassungszusatzes dar, da in diesem Fall keine physische Verletzung der Privatheit stattfände. Eine Verletzung dieses Verfassungszusatzes läge nur vor, wenn „an official search and seizure of his papers or his tangible material effects or an actual physical invasion of his house ‚or curtilage' for the purpose of making a seizure" (Olmstead 1928, 466) statt fände. Langfristig bekannter und einflussreicher als das

Urteil in diesem Fall wurde der *Dissent* von Brandeis, der inzwischen *Supreme Court*-Richter geworden war und – ähnlich wie fast 40 Jahre zuvor in seinem Aufsatz mit Warren argumentierend – feststellte, dass auch das Abhören von Telefonleitungen ein illegales „search and seizure" nach dem *Fourth Amendment* darstelle, auch wenn hierbei nicht physischer, tatsächlich greifbarer Besitz davon berührt sei, sondern „nur" Gespräche (Olmstead 1928, 438). Brandeis postulierte, dass hieraus in der Tat ein „Recht in Ruhe gelassen zu werden" abzuleiten sei.

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. ... They conferred, as against the Government, the right to be let alone the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment (Olmstead 1928, 478f.).

Auch in Olmstead war Brandeis sich dessen bewusst, welchen Einfluss die Entwicklung neuer Technologien auf die Ausformung von Privatheit hat: „Subtler and more far reaching means of invading privacy have become available to the Government", schrieb er. „Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet" (zit. nach Gormley 1992, 1369).

Bis in die 1960er Jahre hinein gab es keine grundsätzlich abweichende Rechtsprechung zu Olmstead. Trotz weitgehender staatlicher Überwachungsmaßnahmen in der McCarthy-Ära bestand offensichtlich gesellschaftlicher Konsens über die Notwendigkeit eingeschränkter Freiheitsrechte angesichts der „kommunistischen Bedrohung". Erst danach begannen sich die Verhältnisse langsam zu ändern: Auf den unteren Gerichtsebenen wurden die ersten abweichenden Urteile zu Verletzungen der Privatsphäre gefällt, es erschienen die ersten Publikationen zum Thema (Westin 1967), und es gab erste Versuche einer gesetzlichen Neuregelung der Telefonüberwachung. Die ersten Untersuchungsausschüsse zu den McCarthy-Exzessen brachten Unerfreuliches zu Tage und unter die Leute. Das gesellschaftliche Klima veränderte sich, und Lyndon B. Johnson erklärte 1967 in seiner *State of the Union Address*: „We should protect what Justice Brandeis called the ‚right most valued by civilized men', the right to privacy" (zit. nach Gormley 1992, 1364).

Die wahrscheinlich wichtigste Entscheidung des *Supreme Court* im Hinblick auf Privatheit und Überwachung erfolgte kurz darauf. Das Urteil im Fall *Katz v. United States* (1967), der sich mit der Rechtmäßigkeit des Abhörens von Gesprächen, die von öffentlichen Telefonzellen aus geführt werden, befasste, betonte: „(T)he constitution protects people not places", und „what a person seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected" (Katz 1967, 351).

> It was not until 1967, in *Katz v. United States*, that the U.S. Supreme Court recognized that the literal transposition of standards, developed to deal with the intrusions encountered in centuries past, was not a viable way by which to preserve and enforce privacy guarantees in an age of electronic communication (Brenner 2002, 135).

Letztendlich hatte sich Brandeis' Idee von Privatheit als „Recht in Ruhe gelassen zu werden" durchgesetzt. Berühmt wurde der Fall Katz aber auch, weil Richter Harlan in seiner Urteilsbegründung schrieb, entscheidend sei eine „reasonable expectation of privacy", also die „begründete Annahme von Privatheit", die er damit als Kriterium für die Bestimmung der rechtlich geschützten Privatheit einführte.

Nach Katz entwickelte der *Supreme Court* zwei Kriterien zur Prüfung dessen, ob eine „reasonable expectation of privacy against intrusions by the government" nach dem Vierten Verfassungszusatz vorliegt: Zunächst muss der/die Einzelne subjektiv glauben, dass das, was er/sie tut, privat sei (das ist die Erwartung), und dann muss ein unbeteiligter Beobachter, z.B. das Gericht, diese Meinung teilen, damit sie als „begründet" gelten kann. In späteren Entscheidungen wurde, ausgehend von Katz, immer wieder darauf hingewiesen, dass Dinge, die sich

sozusagen „im öffentlichen Blick“ befinden, dokumentiert und verbreitet werden dürfen, weil dabei nur bloßgelegt werde, was ohnehin bereits sichtbar sei.

Diese Vorstellung hat zu verschiedenen bemerkenswerten Urteilen geführt. So entschied das oberste Verfassungsgericht 2001 in *Kyllo v. United States*, dass das Aufspüren von Wärmeemissionen (die etwa beim Anbau von Marihuana in Innenräumen entstehen) durch spezielle Messgeräte einer Durchsuchung nahe käme, daher eines richterlichen Durchsuchungsbefehles bedurft hätte und ohne einen solchen eine Verletzung des Vierten Verfassungszusatzes darstelle. Eine große Rolle bei der Begründung spielte die Tatsache, dass die verwendete Technologie neu und „not in general public use“ war und mit ihrer Hilfe Informationen gewonnen wurden, die andernfalls nur durch eine Hausdurchsuchung zu erhalten gewesen wären. Ausgehend von dieser Begründung wird unter JuristInnen aber auch argumentiert, dass die „expectation of privacy“ nicht mehr als begründet gelten könne, sobald eine Technologie hinreichend verbreitet sei – so etwa in einem Fall, wo die Polizei ein Grundstück überflog, womit man nach Meinung des *Supreme Court* zu rechnen habe (*California v. Ciraolo* 1986). Kyllo hat aber nicht, wie von vielen erhofft, zu einer grundsätzlich neuen Bewertung des *Supreme Court* geführt, was das Verhältnis neuer Technologien und den Schutz der Privatsphäre durch den Vierten Verfassungszusatz betrifft. Die Problematik von Privatheit und neueren Technologien, d.h. die Anwendung eines 200 Jahre alten Verfassungszusatzes und seiner – inzwischen auch schon ein halbes Jahrhundert alten – Auslegung durch den *Supreme Court* ist hier vielleicht schon deutlich geworden, vermehrt gilt das auch für Fragen des Schutzes der Privatsphäre im Cyberspace.[6]

Ein wichtiger Aspekt der Interpretation von *Privacy* durch den *Supreme Court* ist die Einschätzung, dass Informationen, die freiwillig an Dritte weitergegeben wurden, nicht mehr vom *Fourth Amendment* geschützt seien. In *United States v. Miller* (1976) hatte der *Supreme Court* argumentiert, dass die Unterlagen eines Kunden bei einer Bank nicht unter diesen Schutz fielen, denn der Kunde habe diese Informationen „voluntarily conveyed to ... banks and exposed to their employees in the ordinary course of business“. Der *Supreme Court* hat in diesem Fall entschieden, dass eine Person bei der Weitergabe ihrer Daten an Dritte „takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government“ (Miller 1976, 442f.). Da also die „reasonable expectation of privacy“ hier entfällt, kann der Staat so, vermittelt über Dritte, auf Daten zugreifen, die sonst dem Schutz der Privatsphäre unterlägen. Diese Einschätzung ist zentral für die Frage der Nutzung von privatwirtschaftlichen Datenbanken für polizeiliche oder geheimdienstliche Ermittlungen, wie Hoofnagle (2004, 622) treffend kommentiert:

> The shortsighted Miller decision does not take into account the reality that individuals need to give their information to third parties in order to participate in society. It is unfair to cede all individuals' rights to a company that can simply hand over personal information to law enforcement. Congress acted swiftly to reverse the Miller decision with respect to financial records, and several state supreme courts have rejected the Miller approach. The current conception of protections under the Fourth Amendment provides individuals with little protection against CDBs (= commercial data brokers; d.A.).

In Folge dieser *Supreme Court*-Urteile hat der Kongress eine Reihe von einzelnen Gesetzen erlassen, die über den verfassungsmäßig vorgeschriebenen Rahmen hinaus die Daten der BürgerInnen vor staatlichem Zugriff sichern sollten. Im folgenden Abschnitt sollen die wichtigsten dieser Gesetze kurz skizziert werden.

3. *Privacy* in der amerikanischen Gesetzgebung

Es gibt in den USA eine Reihe von Gesetzen und *executive orders*, die sich ausdrücklich mit dem Schutz der Privatsphäre und mit Datenschutz beschäftigen. Dazu gehören v.a. der *Privacy Act* (1974) und der *Computer Matching and Privacy Act* (1988). Beide beschäftigen sich ausschließlich mit persönlichen Daten, die sich

im Besitz des Staates befinden, und nicht mit dem Sammeln oder Verwerten von Daten durch private Anbieter. Entstehung und Verabschiedung des *Privacy Act* hängen politisch sehr stark mit Vertrauenskrisen des politischen Systems in den USA nach Watergate bzw. der Ära Nixon zusammen (Westin 2003, 437). Rechtlich steht er in einem direkten Zusammenhang zum Informationsfreiheitsgesetz (*Freedom of Information Act*, kurz FOIA) von 1966. Der *Privacy Act* sollte sowohl Informationen von BürgerInnen in staatlichen Datenbanken schützen, als auch den BürgerInnen ein gewisses (begrenztes) Maß an Verfügungsgewalt über ihre dort gespeicherten Daten geben. Zusätzlich stellt das Gesetz eine unmittelbare Reaktion auf die beginnende technische Entwicklung Computergestützter Datenbanken dar. Grundsätzlich verbietet es die Anhäufung von Daten ohne konkreten Verwendungszweck; werden Daten dennoch erhoben, unterliegt dies einer Reihe von Auflagen, z.B. dass BürgerInnen von der Existenz der Datenbanken unterrichtet werden müssen, dass sie ein Recht haben ihre Daten einzusehen und zu korrigieren, dass die Daten nur für den Zweck verwendet werden dürfen, für den sie erhoben wurden, und dass sie nach einer bestimmten Zeit gelöscht werden müssen. Zentral im *Privacy Ac*t ist die Kategorie der „*fair information practice*", d.h. das Recht Einzelner, Kenntnis darüber zu haben, welche Informationen über sie gespeichert werden und sie gegebenenfalls anzufechten.

> In political terms, a consensus emerged that data banks should not be allowed to consolidate citizen information from separate local or national government agency files, even if this might provide a more complete picture of citizen government relationships (Westin 2003, 437).

Der *Privacy Act* gilt allerdings nur für Daten, die von der Bundesregierung erhoben werden, und für private Gesellschaften, die im Auftrag der Regierung Daten verwalten, d.h. für Daten, die die Regierung erhoben hat und an private Firmen weiterreicht. Im umgekehrten Fall gilt das nicht. D.h. private Datenbankenbetreiber können riesige Datenbanken aufbauen, deren Betrieb dem Staat nach dem *Privacy Act* untersagt wäre. Der Staat wiederum kann dann im Bedarfsfall diese Daten von den privaten Betreibern einkaufen. „At that point, the personal information would be subject to the Privacy Act, but law enforcement and intelligence agencies have special exemptions under the Act that limit access, accuracy, and correction rights" (Hoofnagle 2004, 623). Auch kaufen staatliche Stellen häufig nicht komplette Datensätze ein, sondern lassen auch die Auswertung von Privatfirmen machen, so dass die Daten nicht vom privaten in den öffentlichen Bereich wechseln, d.h. sie bleiben während des gesamten Verfahrens außerhalb des Geltungsbereiches des *Privacy Act*.

1988 wurde der *Computer Matching and Privacy Protection Act* verabschiedet, der den *Privacy Act* ergänzte und sich mit dem Abgleich staatlicher Datenbanken befasst. Die neueren technischen Entwicklungen machten es notwendig gesetzlich zu regeln, wie und unter welchen Bedingungen es dem Staat erlaubt sein sollte Daten, die verschiedene Stellen erhoben hatten, zusammenzuführen oder abzugleichen. Besonders im Bereich der Sozialhilfe oder beim Eintreiben von Bußgeldern wurden Datensätze abgeglichen. Nach dem *Computer Matching and Privacy Protection Act* muss hierfür eine Vereinbarung zwischen den Behörden getroffen werden, in der Zweck und Verfahrensweise des Abgleichs sowie die getroffenen Maßnahmen gegen Datenmissbrauch (durch Dritte) detailliert beschrieben werden. Zwar müssen BürgerInnen nicht grundsätzlich davon informiert werden, dass ihre Daten abgeglichen werden, spätestens aber wenn Entscheidungen auf der Basis von so gewonnenen Informationen getroffen werden, muss der/die Einzelne in Kenntnis gesetzt werden, um gegebenenfalls Einspruch erheben zu können. Ein weiteres Gesetz in diesem Bereich ist der *Computer Security Act* von 1987, der Mindeststandards für die Sicherheit personenbezogener Daten in staatlichen Computern definiert.

Es gibt noch eine Reihe weiterer Gesetze auf Bundesebene, die den *staatlichen Zugriff* auf staatlich erhobene Daten regeln; allen gemein ist, dass sie bestimmte personenbezogenen Daten als vertraulich definieren, Richtlinien für den

Umgang mit diesen vertraulichen Informationen festlegen und Strafandrohungen hinsichtlich der Verletzung dieser Richtlinien formulieren. Zu den Informationen, die als besonders vertraulich geschützt werden, gehören finanzielle Informationen (z.B. durch den *Tax Reform Act*), bildungsbezogene Daten (z.B. durch den *National Education Statistics Act*) und auch Gesundheitsdaten. Gemein ist all diesen Regelungen, dass der staatliche Zugriff auf die Daten durch sogenannte *National Security Letters* geregelt wurde, die dem FBI oder der Polizei den Zugriff unter bestimmten Bedingungen erlauben.

Der Tatsache, dass es so wenige Gesetze gab, die den Umgang mit personenbezogenen Daten im nicht-staatlichen Kontext regeln, lag auch die Vorstellung zugrunde, dass große Datenbanken einen technischen und finanziellen Aufwand erfordern, der letztendlich nur von staatlicher Seite aufzubringen wäre: „Until the rise of the Internet, misuse of personal data held by entities other than the federal government did not command much attention from policymakers as a threat to privacy or personal liberty" (Stratford/Stratford 1998, 19). Einige wenige Gesetze beschäftigen sich dennoch mit dem Umgang Privater mit vertraulichen Daten, zumeist im Bereich der (persönlichen) finanziellen Informationen.

Am bekanntesten unter diesen ist der *Fair Credit Reporting Act* (FCRA), der regelt, wie die „*consumer credit reporting agencies*" mit Daten umgehen dürfen. Hier wird festgelegt, wie welche Daten, für welchen Zweck wie lange gespeichert werden dürfen und es wird auch hier dem/der BürgerIn ein gewisses Maß an Einfluss gewährt – er/sie hat das Recht Kenntnis darüber zu erhalten, was gespeichert wird und die Angaben gegebenenfalls zu korrigieren. „The Fair Credit Reporting Act (FCRA) was the first federal law to regulate private-sector use and disclosure of personal information. It offers the greatest opportunities for protection of data held by CDBs" (Hoofnagel 2004, 623). Nach derzeitiger Interpretation ist der FCRA jedoch nur dann anwendbar, wenn die Daten benutzt werden, um die persönlichen Voraussetzungen bei der Vergabe von Krediten und Stellen oder beim Abschluss von Versicherungen zu prüfen. Wenn die von den „*consumer credit reporting agencies*" gesammelten Daten für andere Zwecke (z.B. Terroristenfahndung) eingesetzt werden, unterliegen sie nicht dem Schutz nach dem FCRA (Dempsey/Flint 2003, 6).

Vor ca. 15 Jahren begann ein Umdenken und zunehmend wurde auch der Schutz der Privatsphäre vor nicht-staatlichen Übergriffen diskutiert (Westin 2003, 444f.). Seit den späten 1990er Jahren gab es eine Reihe von Gesetzesinitiativen auf Bundes- wie einzelstaatlicher Ebene, den Datenschutz im privatwirtschaftlichen Bereich zu stärken, wobei besonders Fragen des Datenschutzes im Zusammenhang mit *eCommerce* im Vordergrund standen. Dennoch blieben auch diese Initiativen Flickwerk, weil sie sich auf jeweils eng gefasste Bereiche konzentrierten. Hierzu gehören z.B. 1998 der *Children's Online Privacy Act* zum Schutze von Kindern im Internet und 1999 das erste Bundesgesetz zum Schutz der finanziellen Privatsphäre (im Rahmen des *Gramm-Leach-Bliley Financial Services Modernization Act*). Es folgten der *Health Insurance Portability and Accountability Act* und unzählige Gesetze und Gesetzesinitiativen auf einzelstaatlicher Ebene.

> Legislation was pending in Congress and state legislatures concerning financial privacy, medical privacy, employee privacy, online privacy, the use of Social Security Numbers, protection against identity theft, and other privacy related subjects (Cate 2001, 11).

Der 11. September stoppte all diese Entwicklungen. Allein schon die Tatsache, dass sämtliche Gesetzgebungsinitiativen zum Schutze der Privatsphäre zum Erliegen kamen, macht klar, wie sehr sich die amerikanische Einstellung zu *Privacy* unmittelbar danach gewandelt hat.[7] Deutlich wird aber auch, wie problematisch ein nicht verfassungsmäßig verankerter Datenschutz ist: Die über die Verfassung hinausgehende Gesetzgebung kann im Falle politischer Veränderungen – wie eben dem 11. September – im Namen aktueller Sicherheitsinteressen auch wieder zurückgenommen werden. Genau dies ist in den USA im Rahmen der Sicherheitspaketes nach den Anschlägen geschehen.

4. *Privacy* und der *USA PATRIOT Act*

Bis heute zentral für die veränderte Lage von *Privacy* in den USA ist das kurz nach den Anschlägen vom 11. September 2001 verabschiedete Sicherheitspaket *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act)*,[8] ein von *Attorney General* John Ashcroft eingebrachtes Paket von Gesetzen, deren Ziel das Gewinnen neuer Informationen durch vermehrte Überwachung, der erleichterte Austausch von Informationen zwischen Polizei und Geheimdiensten sowie der vereinfachte Zugriff auf existierende Datenbestände war. Im *PATRIOT Act* ist eine große Anzahl von Möglichkeiten verankert, wie Ermittlungsbehörden auf bisher nicht oder nur schwer zugängliche Daten zugreifen können. Konkret heißt das, dass durch den *PATRIOT Act* die vorhandenen rechtlichen Hindernisse, auf Daten zuzugreifen, verringert werden und die bestehende *Privacy*-Gesetzgebung aufgeweicht wird (Chang 2001).

Eines der Einfallstore für diese Aufweichung sind die so genannten *National Security Letters*,[9] mit denen das FBI unter Berufung auf die nationale Sicherheit dann doch auf vertrauliche Daten zugreifen kann. Alle erwähnten Gesetze zum Schutze der Privatsphäre vor staatlichen Übergriffen enthalten bereits Ausnahmeregelungen in unterschiedlichem Umfang, die den Zugriff auf Daten im Zuge polizeilicher und geheimdienstlicher Ermittlungen in dieser Form erlauben. Diese *National Security Letters* mussten jedoch vom *Attorney General* oder seinem Stellvertreter ausgestellt werden, sie mussten auf einzelne Verdächtige bezogen sein und ausreichend begründet werden.

Im *PATRIOT Act* wird in Abschnitt 505 (*Removing Obstacles to Investigating Terrorism*) die Ausstellung und der Geltungsbereich der *National Security Letters* neu geregelt.[10] Nun dürfen sie auch einfache FBI-Beamte ausstellen und damit die Herausgabe von Unterlagen verlangen. Die Unterlagen müssen auch nicht mehr im Kontext einer konkreten Ermittlung stehen, sondern es reicht, dass sie „relevant" sind für eine „authorized investigation to protect against international terrorism or clandestine intelligence activities."

Diese Veränderungen im Bereich *National Security Letters* wirken sich u.a. auf den Zugriff auf Unterlagen der Telephongesellschaften und Internetbetreiber aus. Der *Electronic Communications Privacy Act* (ECPA) erlaubt es jetzt, dass das FBI mit einem Stück Papier, das lediglich von dem/der zuständigen Beamten im Einsatz unterzeichnet ist, von der Telephongesellschaft oder vom Internetprovider ohne begründeten Verdacht Verbindungsdaten verlangen kann, vorausgesetzt, diese sind in irgendeiner Weise „relevant". Zu den Informationen, die das FBI so bekommen kann, gehören die IP-Adresse des/der Jeweiligen, alle IP-Adressen sämtlicher Webserver, mit denen kommuniziert wurde, Identitäten aller Personen, die Email von dem/der Betroffenen erhalten haben oder von denen der/die Betroffene Email bekommen hat. Uhrzeit, Umfang in Bytes und Dauer aller Online-Aktivitäten und alle Seiten, die besucht wurden, gehören ebenfalls zu den Daten, auf die so zugegriffen werden kann.[11]

Mit ähnlichem Prozedere können finanzielle Daten abgefragt werden. Der oben erwähnte *Fair Credit Reporting Act* wird durch den *PATRIOT Act* ergänzt um eine Bestimmung (Abschnitt 626), die es jetzt *jeder* staatlichen Stelle mit der Begründung, die Informationen seien in irgendeiner Weise relevant für die Ermittlungen, Aktivitäten oder Analysen im Kampf gegen den Terrorismus, erlaubt, auf komplette „*credit files*" zurückzugreifen. Noch bleibt unklar, ob die staatlichen Stellen einzelne KonsumentInnen spezifizieren müssen oder ob sie pauschalen Zugang zu allen Unterlagen, oder zumindest all denen, die bestimmte Merkmale aufweisen, verlangen können.

Auch die Ausbildungsdaten der AmerikanerInnen sind jetzt dem FBI vereinfacht zugänglich. Der *Family Educational Rights and Privacy Act* wird durch den *PATRIOT Act* (Abschnitt 507) ergänzt, der es gleichfalls Ermittlungsbehörden erlaubt, auf die entsprechenden Daten zuzugreifen, wenn sie „relevant" sind für die Terrorismusbekämpfung.

Zusätzlich gilt auch hier das Geheimhaltungsgebot: Firmen, die wegen *National Security*

Letters Informationen weitergeben mussten, dürfen dies nicht bekannt machen, d.h. die Einzelnen nicht davon unterrichten, dass ihre Daten weitergegeben wurden. Die Kenntnis der von den Privaten so erhaltenen Informationen bleibt auch nicht auf das FBI beschränkt: Explizit wird ihm erlaubt, so gewonnene Erkenntnisse mit anderen Behörden (z.B. der CIA) zu teilen.

Neben dem Zugriff durch *National Security Letters* kann sich das FBI nach dem *PATRIOT Act* (Abschnitt 215) mit Hilfe des *Foreign Intelligence Surveillance Act* (FISA) auch Geschäftsunterlagen aller Art beschaffen. Auch hier ist es jetzt möglich, bei Terrorismusermittlungen ohne genaue Nennung der Zielperson einen richterlichen Beschluss für Geschäftsunterlagen zu erhalten, d.h. theoretisch kann auf ganze Datenbanken zugegriffen werden. Die Überwachungen und Durchsuchungen nach FISA wurden 1978 unter Carter etabliert. FISA sieht sehr viel geringere Hürden für die Genehmigung von Abhöraktionen oder Durchsuchungen vor, weil es sich nicht um polizeiliche Ermittlungen, sondern lediglich um nachrichtendienstliches Sammeln von Informationen handelt. Durch die Erweiterung der Definition dessen, was es heißt, im Dienst einer fremden Macht zu stehen, kann FISA jetzt auch bei strafrechtlichen Ermittlungen eingesetzt werden.

Zusätzlich zu den neuen Zugriffsmöglichkeiten hat die Regierung auch die Auflage für Firmen geschaffen, bestimmte Daten zu sammeln und zu speichern und an staatliche Stellen entweder routinemäßig oder auf Anfrage weiterzuleiten. Die Grundlage ist auch hier vor dem *PATRIOT Act* angelegt: in diesem Fall im *Bank Secrecy Act* von 1970, der zur Verhinderung von Geldwäsche Banken verpflichtete, verschiedene Transaktionsdaten an den Staat weiterzuleiten. Um diesen neuen Verpflichtungen entsprechen zu können, werden inzwischen bereits Softwaretools angeboten, z.B. für Geldinstitute, die damit – wie die Werbung verheißt – „*PATRIOT Act* kompatibel" werden können.

Die Entwicklung hin zur Aushöhlung bestehender *Privacy*-Gesetzgebung ist aber sicherlich noch nicht abgeschlossen. Auch in der deutschen Presse wurde der Versuch der Regierung Bush, ein weiteres Sicherheitspaket auf den Weg zu bringen, breit kommentiert. Dieses Gesetzespaket, als *PATRIOT II* bezeichnet, gelangte durch eine gezielte Indiskretion im September 2003 an die Öffentlichkeit und wurde – nach heftigen öffentlichen Protesten – zurückgezogen.[12] Aber dies war nur ein begrenzter Erfolg: Ein Teil von *PATRIOT II* wurde daraufhin in einem anderen Gesetz, dem *Intelligence Authorization Act for Fiscal Year 2004*, durchgeschleust. In diesem jährlichen Standardgesetz zur finanziellen Ausstattung der Geheimdienste wurden die Überwachungsbefugnisse des FBI nochmals erweitert und z.B. die Definition von „*financial institution*" ausgedehnt, so dass sie jetzt u.a. Reisebüros, Makler, die Post, Versicherungen, Spielbanken und Autohändler umfasst.

Zusätzlich versuchte die Regierung Bush im Sommer 2004 mehr oder minder unauffällig einen weiteren Teil von *PATRIOT II* durchzubringen, nämlich im *Anti-Terrorism Intelligence Tools Improvement Act of 2003*. Mit diesem Gesetz sollen Teile des *PATRIOT Act* entfristet und die Überwachung nach FISA noch stärker ausgeweitet werden. FISA soll nun auch anwendbar sein auf Einzelpersonen, denen weder Kontakte zu TerroristInnen noch zu fremden Nationen nachgewiesen werden kann. Zusätzlich sollen Ergebnisse solcher FISA Aktionen bei Einbürgerungs- und Visa-Erteilungsverfahren (und natürlich bei Ausweisungs- und Deportationsverfahren) verwendet werden, ohne den/die Betroffene/n davon in Kenntnis zu setzen. Das ist nach dem *Alien Terrorist Removal Proceedings Act* von 1996 (Abschnitt 1531–1537) bei erwiesenen TerroristInnen heute schon möglich, nach dem neuen Gesetz bliebe dies aber eben nicht nur auf tatsächliche TerroristInnen beschränkt. Ein weiterer wichtiger Bestandteil des *Anti-Terrorism Intelligence Tools Improvement Act of 2003* ist die Erhöhung des Strafmaßes für Personen, Organisationen und Betriebe, die ihrer Auskunftspflicht nach den *National Security Letters* nicht nachkommen oder die Schweigepflicht verletzen und über entsprechende Ersuchen des FBI Dritte in Kenntnis setzen. Aus all diesem wird deutlich, dass die Bedrohung der Privatheit durch immer neue Sicherheitsgesetze noch lange nicht zum Abschluss gekommen ist.

5. *Privacy* und die neue Datenaufbereitung und -auswertung

Die erweiterten Überwachungsmöglichkeiten, wie sie der *PATRIOT Act* bietet und die in den USA – und inzwischen auch in Deutschland – verschiedentlich diskutiert worden sind, beziehen sich allerdings nicht nur auf die Erhebung von Daten, sondern auch auf deren Auswertung. Um die Dimensionen dieser neuen Datenauswertung deutlich zumachen, soll zunächst skizziert werden, was eigentlich das qualitativ Neue daran ist.

Traditionelle Datenüberwachung sammelt Informationen über einzelne identifizierbare Individuen, an denen ein Überwachungsinteresse besteht. Im Ergebnis entsteht eine „collection of information about an identifiable individual, often from multiple sources, that can be assembled into a portrait of that person's activities" (Stanley/Steinhardt 2003, 3). Privatwirtschaftlich wird dies z.B. häufig bei der Überprüfung von Kreditnehmern oder potentiellen MieterInnen genutzt. Entsprechende Datenbanken werden von Firmen wie *ChoicePoint* oder *Seisint* angeboten.[13] Auch die Rasterfahndung gehört noch zu den „traditionelleren" Methoden der Datenüberwachung. Ihr Ziel ist es, eine (ermittlungstechnisch) zu bewältigende Menge von Personen mit bestimmten, zuvor identifizierten Charakteristika aus einer (nahezu) unbegrenzten Menge zu isolieren. Hierbei werden mindestens zwei Datensätze (die aus unterschiedlichen Datenquellen stammen können) miteinander korreliert. Die dadurch sichtbare Schnittmenge genügt entweder selber bereits den Ermittlungsanforderungen, oder es werden auf Basis dieser Auswahl andere Ermittlungsmethoden eingesetzt.

Zur Umsetzung solcher „traditioneller" Überwachungs- und Suchtechniken sind vor allem große zentralisierte Datenbanksysteme zu implementieren. Praktisch alle biometrischen Überwachungstechniken, die im *War on Terrorism* eingesetzt werden sollen – von Iris Scans bis zur DNA-Analyse –, gehören in den Bereich der Personenidentifizierung und -authentifizierung. Sie ergeben nur dann wirklich einen Sinn, wenn möglichst alle EinwohnerInnen des Landes mit den jeweiligen Merkmalen in Datenbanken erfasst sind. Solange dies nicht machbar – weil noch nicht politisch durchsetzbar – ist, begnügen sich die Ermittlungsbehörden mit Daten von Nichtstaatsbürgern, die bei der Vergabe von Visa oder bei der Einreise erfasst werden.

Grundsätzlich werden auch alle Ergebnisse anderer Formen von Überwachung ebenfalls digitalisiert und über Datenbanken erschlossen. Es entstehen also immer größere staatliche Datenbanken. Nicht alle Daten sind dabei notwendigerweise das Resultat technologisch hochentwickelter Überwachung. Es gibt auch den großen Bereich dessen, was Froomkin (2000) „*routinized low-tech data collection*" nennt, nämlich Daten, die der Staat routinemäßig erhebt, z.B. im Zusammenhang mit den jährlichen Steuererklärungen und mit dem alle zehn Jahre durchgeführten Zensus.[14] Die einzelnen Bundesstaaten sammeln z.B. Daten bei der Ausstellung von Führerscheinen – da fast jede/r erwachsene US-BürgerIn einen Führerschein hat, sind das wahrscheinlich die umfassendsten Datenbanken der USA. Auch im Gesundheitswesen entstehen ohne elaborierte Überwachungstechnologien große Mengen an persönlich zuordenbaren Daten: Krankenversicherungen, Krankenhäuser, Arztpraxen generieren alle Daten, die in den USA nach dem *Health Insurance Portability and Accountability Act* von 1996 erfasst werden. Weitere umfassende Datenbanken werden vom *Department of Education* betrieben; auf Erschließung all dieser Daten zielen die entsprechenden Passagen des *PATRIOT Act*.

Hinzu kommt die in den letzten 25 Jahren enorm angewachsene Menge an privaten Daten: Fast alle kommerziellen Aktivitäten werden digital erfasst und gespeichert; bargeldloses Einkaufen, Online-Bestellungen, Kundenkartennutzung, Besuche von Websites, Abonnieren von Zeitschriften und Newsletters – all diese Aktivitäten hinterlassen eine Spur von digitalen Daten, die immer umfassender wird.

> Our physical bodies are being shadowed by an increasingly comprehensive ‚data body'. However, this shadow body does more than follow us. It also precedes us. Before we arrive somewhere, we have

> already been measured and classified. Thus, upon arrival, we're treated according to whatever criteria have been connected to the profile that represents us (Stalder 2002, 121).

Diese Daten werden gespeichert, analysiert und auch verkauft – und zunehmend gehört der Staat zu den Käufern. Was nicht nur die verfügbare Datenmenge erhöht, sondern es dem Staat auch gleichzeitig möglich macht Daten, die er nach dem *Privacy Act* von 1974 nicht erheben darf, einfach käuflich zu erwerben.

Der staatliche Zugriff auf privatwirtschaftlich erhobene Daten ist auf unterschiedlichen Wegen möglich, zum Beispiel durch die freiwillige Überlassung von (Kunden)Daten. Bekannt geworden ist hier v.a. die freiwillige Herausgabe von Passagierdaten durch amerikanische Fluggesellschaften, wie z.B. dem Billiganbieter *JetBlue Airways*, der dem *Defense Department* freiwillig entgegen seinen eigenen Datenschutzrichtlinien die Daten von über fünf Mio. Passagieren überlassen hat (o.A. 2003). Außerdem gibt es jene Fälle, in denen der Staat auf privatwirtschaftlich entstandene Daten Anspruch erhebt durch eben die Gesetze, die bisher genannt wurden und die meistens ursprünglich im Kampf gegen Geldwäsche oder Drogenhandel entstanden (Arzt 2004). Auf einigen Gebieten müssen Firmen Daten speichern, die sie selber nicht benötigen, nur um sie dem Staat gegebenenfalls zur Verfügung stellen zu können.

Ein Projekt, das besondere Aufmerksamkeit erregte, ist CAPPSII (*Computer Assisted Pre-Passenger Screening*). Die *Transportation Security Administration* (TSA) – inzwischen ein Teil des *Department of Homeland Security* – unterhält eine Datenbank, in der Personen gespeichert werden, die ein potentielles Risiko für die Sicherheit des Luftverkehrs darstellen. Auch hier werden die Probleme der Verknüpfung privater und staatlicher Daten deutlich. So hat *Northwest Airlines* nach dem 11. September Millionen von Passagierdaten an die TSA weitergegeben, die die Informationen mit Daten aus dem 1990 U.S. Zensus abglich.

Schließlich gibt es Fälle, in denen der Staat Daten, die er zu Ermittlungszwecken zu brauchen meint, käuflich von privaten Datenanbietern erwirbt. Dies sind größtenteils privatwirtschaftlich generierte Daten, aber teilweise auch staatliche, wie z.B. Gerichtsakten oder Grundbucheinträge, die aber staatlicherseits nirgendwo zentralisiert verwaltet werden.

> Much of the personal information made available to law enforcement originates from public records. In a variety of contexts, the government compels individuals to reveal their personal information, and then pours it into the public record for anyone to use for any purpose. The private sector has collected the information, repackaged it, and brought it back to the government full circle (Hoofnagle 2004, 634).

Die Firmen, die diese Daten anbieten, verkaufen dem Staat dabei nicht einfach irgendwelche Datensätze, sondern bauen die Datenbanken gleich entsprechend für den staatlichen Bedarf auf: „The sale of personal information goes far beyond simply making the data available to government. ChoicePoint and others tailor their data for law enforcement agencies" (Hoofnagel 2004, 611).[15]

Solch heterogenen, in unterschiedlichen Formaten gespeicherten Daten aus staatlichen und privatwirtschaftlichen Quellen in zusammenhängende Datenbanksysteme zu integrieren, ist eine komplexe Aufgabe. Diese Form der Speicherung und Verwaltung wird auch *data warehousing* genannt, und die neuen Programme der US-Regierung nach dem 11. September betreffen teilweise zunächst einmal den Auf- und Ausbau solcher „Datenlager". Darüber hinaus sollen aber auch durch die Programme neue Analyse-*tools* entwickelt und zur Anwendung gebracht werden.

Der zentrale Begriff bei der schnellen – und kostengünstigen – Auswertung dieser riesigen Datenmengen ist *data mining*. In den Medien werden „*data mining*", „*data surveillance*" oder „*dataveillance*" häufig synonym verwendet. *Data mining* im engeren Sinne ist aber etwas anderes als traditionelle Datenüberwachung, nämlich das Suchen nach verborgenen Mustern in vorhandenen Datensammlungen. In einem Bericht des *Government Accounting Office* (GAO) vom Mai 2004 wird *data mining* definiert als „the application of database technology and techniques – such as statistical analysis and modeling – to uncover hidden patterns and

subtle relationships in data and to infer rules that allow for the prediction of future results" (GAO 2004, 4). Es geht also dabei um automatisierte Verfahren, mit denen aus sehr großen Datenbanken Informationen extrahiert werden, um darin Zusammenhänge und Muster aufzudecken, die der/die BenutzerIn vorher nicht explizit definiert hat.

Die mathematischen, statistischen und informationstechnischen Methoden, die beim *data mining* verwendet werden – z.B. künstliche neuronale Netzwerke, Entscheidungsbäume, Bayes'sche Inferenznetzwerke, genetische Algorithmen und andere Methoden der explorativen Datenanalyse wie z.B. Datenvisualisierung – stammen teilweise bereits aus den 1980er und 1990er Jahren und wurden in einer Vielzahl von Anwendungsfeldern von der Biologie über Finanzmathematik bis hin zur Teilchenphysik eingesetzt. Allen gemein ist, dass sie versuchen, Antworten auf noch nicht formulierte Fragen zu finden bzw. Prognosen oder mögliche Szenarien zu entwickeln. Zumindest der Theorie nach sind diese Verfahren umso Erfolg versprechender, je umfangreicher und vielfältiger die zur Verfügung stehenden Daten sind. Je größer die Datenmenge ist, desto eher sind auch geringere Abweichungen als „*pattern*" identifizierbar. *Data mining* ist damit nicht nur ein Mittel, mit großen Datenmengen umzugehen, sondern selbst ein Motiv, große Datenbanken zu schaffen.

Die Verwendung von *data mining* ist in den letzten Jahren denn auch exponentiell gestiegen, einerseits durch die Mengen an Daten, die täglich erfasst werden, und andererseits durch die gewachsenen technische Möglichkeiten (Rechen- und Speicherkapazitäten, Entwicklung von Software Programmen (*data mining tools*)). Heute können Daten unterschiedlichster Formate und Inhalte (Text-, Multimedia-, Transaktions-, räumliche Daten) beim *data mining* verwendet werden. Zumindest in der Durchführung, wenn auch vielleicht nicht in der Entwicklung, ist *data mining* weniger kostenintensiv als alle traditionellen Formen der Überwachung. Es ist daher nicht länger nötig sorgfältig abzuwägen, wer oder was überwacht werden soll (Clarke 1997).

Beim *data mining* geht es nicht darum, einfach einen schnelleren, weil digitalisierten, Zugriff auf bereits vorhandene Informationen zu schaffen. Vielmehr entsteht tatsächlich etwas qualitativ Neues. Das Bild vom Suchalgorithmus als Bergmann (*miner*), der die verborgenen Informationen zu Tage fördert, führt daher in die Irre: Es handelt sich eher um den Alchemisten, der aus verschiedenen disparaten Elementen versucht, etwas Neues zu schaffen – ob nun Gold oder Katzengold, sei erst einmal dahingestellt. Durch die Kombination und Rekombination von Daten und die Analyse durch *data mining tools* entstehen umfassende Personenbilder – Stalders „*data bodies*" –, die eine neue Qualität der Verletzung von *Privacy* darstellen.

Zusammen stellen *data warehousing* und *data mining* die ideale Neuauflage eines alten Kontrollparadigmas dar. Denn nach dem 11. September hat sich – übrigens auch in Deutschland – das Interesse der Sicherheitsbehörden deutlich von der Strafverfolgung in Richtung auf die Prävention von Straftaten verschoben. Es soll nicht mehr ein/e vorher identifizierte/r Einzelne/r überwacht werden (um ihm oder ihr eine Straftat nachzuweisen), sondern es wird eine größere Gruppe überwacht – die nach der Kapazität moderner Datenbanken nahezu beliebig groß sein kann –, deren Mitglieder möglicherweise etwas tun *könnten*. Diese Schwerpunktsetzung auf Massenüberwachung hat sicherlich auch damit zu tun, dass die Anschläge vom 11. September nicht als konkrete Taten individueller Täter, sondern als Ausdruck eines (terroristischen) Zeitgeistes wahrgenommen und dargestellt wurden (Lepsius 2002, 3f.). Die Preisgabe der Unschuldsvermutung stellt insgesamt eine stärkere Gefährdung von *Privacy* dar als alle neuen technischen Mittel, die im Rahmen der eher traditionellen Überwachung eingesetzt werden.

5.1. Privacy *und* Datamining-*Initiativen der US-Regierung nach dem 11. September*

Total Information Awareness – Nach dem *PATRIOT Act*, der u.a. neue Formen der Über-

wachung und neue Formen der Zusammenarbeit zwischen unterschiedlichen Sicherheitsbehörden ermöglicht, sind Projekte in den Vordergrund gerückt, die bei der Prävention und Aufklärung terroristischer Aktivitäten auf *data mining* setzen. Das erste Beispiel hierfür war das *Total Information Awareness*-Projekt (TIA), das als Zusammenführung bestehender staatlicher und privatwirtschaftlicher Datenquellen zu einer großen, zentralisierten nationalen Datenbank geplant war. Zu den Informationen, die hier kombiniert und korreliert werden sollten, gehörten „bank records, tax returns, driver's license data, credit card purchases, airline tickets, gun purchases, work permits, and more" (Ramasastry 2002).

Im Rahmen von TIA sollten vor allem aber auch Programme entwickelt werden, die neue Möglichkeiten im Bereich der Datenanalyse und -auswertung eröffnen würden. In einem Bericht zu TIA (DARPA 2003) wurden verschiedene Programme vorgestellt, wie *Global Autonomous Language Exploitation*, das Computern ermöglichen sollte, aus Rohdaten eigenständig Berichte zusammenzustellen, die den Interessen des Auftraggebers entsprechen, die aus seinen vergangenen Aktionen abgeleitet werden sollten. *Scalable Social Network Analysis* sollte durch die Verknüpfung von sozialen Interaktionen, finanziellen Transaktionen, Telefongesprächen und Mitgliedschaften in Organisationen die Modellierung und Charakterisierung menschlicher Beziehungsnetzwerke ermöglichen. *MisInformation Detection* sollte durch den Abgleich von Daten in größeren Datenmengen Fehlinformationen und Widersprüche identifizieren. Hierbei sollten linguistische Verfahren, Selbstlernprozesse, Ablaufanalysen von Geschäftsprozessen, deduktive Erkennung von Unregelmäßigkeiten, wissensbasierte und bayesianische Schlussfolgerungen in die Entwicklung einfließen. Zusätzlich gab es eine Reihe von Projekten im Bereich biometrischer Identifizierung und Authentifizierung etc.

TIA hatte von Anfang an einen schlechten Start: Ob es der Name war, der etwas Orwellsch anmutete, oder das seltsame Logo mit Auge und Pyramide, das aussah wie aus dem Traum eines Verschwörungstheoretikers, oder die Nominierung von John Poindexter als Direktor – irgendwie hinterließ TIA keinen guten Eindruck. Zwar gab es schon bald Bemühungen, die Anfangsfehler auszubügeln – das Logo verschwand sang- und klanglos, und im Mai 2003 wurde auch der Name von *Total Information Awareness* in „*Terrorism Information Awareness*" geändert –, aber so richtig half das nichts. Aufgrund alarmierender Berichte – u.a. von der *American Civil Liberties Union* (ACLU) – wurde im Januar 2003 eine Gesetzesvorlage von den Senatoren Russ Feingold (Wisconsin) und Ron Wyden (Oregon) „*Limitation on Use of Funds for Research and Development on Total Information Awareness Program*" angenommen, die ein einstweiliges Einfrieren aller TIA-Gelder bis zur Fertigstellung eines Berichtes für den Kongress über die Einzelprojekte vorsah. Der Bericht soll vor allem auch bürger- und datenschutzrechtliche Fragen zu einzelnen TIA-Bestandteilen klären. TIA versuchte, Boden gut zu machen, und richtete im Februar 2003 ein internes Aufsichtsgremium und eine externe Beratungskommission ein, die sich mit *Privacy*-Fragen beschäftigen sollten. Der dem Kongress im Mai 2003 vorgelegte Bericht ging auch auf bürgerrechtliche Bedenken ein und benannte Schutzmechanismen, die entwickelt werden sollten, um eine missbräuchliche Verwendung von Daten zu verhindern. Auch die Schutzmechanismen sollten wieder automatisiert werden, um Transgressionen selbsttätig erkennen und verhindern zu können.

Trotz aller Bemühungen von TIA, „salonfähig" zu werden, beschlossen Senat und Kongress im September 2003, das Programm endgültig zu stoppen, wobei datenschutzrechtliche Bedenken die zentrale Rolle spielten. Es wurde nicht nur die Finanzierung der TIA-Programme eingestellt, sondern es wurde außerdem verfügt, dass bestehende Komponenten von TIA nur an andere Behörden oder Ministerien zur Implementierung weitergegeben werden dürften, wenn der U.S. Kongress darüber informiert worden sei und seine Zustimmung erteilt habe. Lediglich bei Auslandseinsätzen und bei Spionage gegen „non-United States persons" können TIA-Programme weiterhin eingesetzt werden. Die weitere Forschung in den entsprechen-

den Bereichen ist im Gesetz nicht ausdrücklich untersagt.

MATRIX – Die Einstellung der TIA-Programme durch Senat und Kongress nach erfolgreichen Kampagnen der Bürgerrechtsorganisationen sah zunächst nach einer großen Erfolgsgeschichte und dem Sieg demokratischer Grundwerte gegen staatliches *data mining* aus, aber bei genauerem Hinsehen scheint die Freude verfrüht: Nachdem deutlich wurde, dass in nächster Zeit auf Bundesebene keine Unterstützung für zentrales *data mining* zu erwarten war, wurden diese Programme z.T. auf die Ebene der Einzelstaaten verlagert. Ein Verbund von ursprünglich elf Bundesstaaten – Connecticut, Michigan, New York, Ohio, Pennsylvania, Alabama, Florida, Georgia, und Utah – beauftragte die Firma *Seisint* in Florida, ein *data mining*-Programm zu entwickeln. Dieses Programm, genannt MATRIX *(Multistate Anti-Terrorism Information Exchange*), verknüpft alle Datensätze zu einer Person, die sich in staatlichen Datenbanken befinden (z.B. Strafregister, Führerschein, Kfz-Zulassungen, Haftunterlagen und digitalisierte Photos), und macht sie den angeschlossenen Polizei- und Geheimdienstbehörden zugänglich. Der Datenbestand wird durch den Ankauf von Datensätzen kommerzieller Datenbankbetreiber ergänzt. *Seisint* hat in einer Informationsveranstaltung angegeben, dass das System zur Zeit 20 Milliarden Daten aus über 100 verschiedenen (z.T. privatwirtschaftlichen) Datenbanken anbietet. Die eingesetzte Datenanalyse-Technik sollte es erlauben, zu jedem beliebigen Suchmuster ohne Zeitverlust ein Ergebnis zu erhalten.

Auch MATRIX sah sich, sobald es bekannter wurde, heftiger Kritik ausgesetzt. Beanstandet wurde vor allem, dass es lediglich nominell ein *state program* sei, tatsächlich aber Gelder aus Washington erhielt, nämlich vom U.S. Justizministerium und dem *Federal Department of Homeland Security*, dem auch Kontrollmöglichkeiten eingeräumt wurden. Der Vorwurf wurde laut, es handle sich hierbei um eine bewusste Umgehung der Restriktionen des Kongresses im Bereich *data mining*. Eine weitere Zielscheibe der Kritik war – ähnlich wie bei TIA und John Poindexters Iran-Contragate-Vergangenheit – die Person des Firmeninhabers Hank Asher, der offensichtlich ein ehemaliger Drogenschmuggler war, was manchen nicht ganz die richtige Qualifikation für einen Sicherheitsjob zu sein schien. Interessanter an Ashers Vergangenheit ist aber eigentlich ein anderer Punkt: Seine frühere Firma (die er später an *ChoicePoint* verkaufte) war in Florida beteiligt an der – teilweise fehlerhaften – Erstellung von Wählerlisten, die WählerInnen von der letzten Präsidentschaftswahl ausschloss (Rötzer 2003).

Seisint bot bereits kurz nach den Anschlägen den Behörden völlig uneigennützig einen Datenbestand von 120.000 EinwohnerInnen der USA mit einem so genannten „*High Terrorist Factor*" an. Die Faktoren, aus denen *Seisint* diesen Terrorismus-Quotienten errechnete, waren: Alter und Geschlecht, Führerschein, Pilotenschein oder Beziehungen zu Piloten, Nähe zu „*dirty addresses/phone numbers*", Strafregister, wie sie postalische Sendungen erhielten oder verschickten, Anomalien in ihren Sozialversicherungsnummern, finanzielle Transaktionen und ethnische Herkunft.

Allgemein wurde kritisiert, dass MATRIX erneut Informationen von BürgerInnen aus staatlichen und privatwirtschaftlichen Datenbanken kombiniert und dann Regierungsbeamten zur Verfügung stellt, die in Millionen von Datensätzen nach „Anomalien" suchen könnten, die auf terroristische oder andere kriminelle Aktivitäten hinweisen. Es handelt sich also um ein *data mining*-Projekt, wie auch der Direktor der Abteilung *Technology and Liberty* der ACLU feststellte:

> Supporters of this system have claimed that it does nothing more than make existing everyday police activities more efficient. We now know that is not the case. This is data mining pure and simple: the authorities compile information from numerous public and private sources and let a computer decide if you're a threat. That capability is completely unprecedented in our history, and remains unrestrained by our legal system (ACLU 2004a).

Insgesamt setzt die Kritik am *data mining* in den USA allerdings zumeist an den Widersprüchen der Realisierung an, so an der teilweise rassistischen oder diskriminierenden Praxis,

denn Herkunftsländer, Religionszugehörigkeit oder Hautfarbe sind häufige Ausgangsparameter. Es ist auch bemerkt worden, dass es sich um ein gerade bei der Bekämpfung von Terrorismus vielleicht wenig effektives Mittel handelt, da sich TerroristInnen nach Aussagen des FBI eben dadurch auszeichnen, *nicht* auffällig zu sein. Das FBI hat daher auch „longtime citizens ... who may not have anything unusual in their immediate history" als Fahndungsziele definiert und interessiert sich somit für „all parts of the muslim community" (AP-Meldung vom 12. Juli 2002). Ein weiterer Kritikpunkt ist die Gefahr der Verdächtigung Unschuldiger, entweder aufgrund fehlerhafter Daten oder einer Fehlinterpretation korrekter Daten. Dieses Problem der falschen positiven Identifizierung ist besonders kritisch, da die Betroffenen meist von der Existenz der Datenbanken oder der durchgeführten *data mining*-Verfahren keine Kenntnis und so auch keine Möglichkeit haben, Widerspruch einzulegen.[16]

Zukünftige Programme – Auch im Falle von MATRIX scheint der Protest der Bürgerrechtsorganisationen – allen voran der ACLU – dazu zu führen, dass das Programm reduziert wird. Inzwischen haben etliche Bundesstaaten – bis auf Florida, Connecticut, Ohio, Michigan und Pennsylvania – ihre Teilnahme an dem Programm eingestellt. Dennoch heißt auch dies nicht, dass es keine *data mining*-Programme mehr gibt. Ein auf Anfrage von Russ Feingold erstellter Bericht des *Government Accounting Office* (GAO 2004) vom Mai diesen Jahres belegt, dass zur Zeit in 199 staatlichen Programmen *data mining* durchgeführt wird. 54 dieser Programme verwenden dafür auch privatwirtschaftlich erhobene Daten. Vier dieser Programme wurden von der ACLU besonders kritisiert, aber auch zu den anderen Programmen wurde kritisch bemerkt, dass nicht klar ist, wie sie ihre Daten verwenden:

> Statistical analysis itself is of course not the problem. It is the construction of systems that systematically aggregate information about the private activities of innocent individuals on a mass scale, and the computerized scrutiny of those activities for allegedly suspicious patterns that is at issue (ACLU 2004b).

Weiterhin gibt es mehrere Versuche, größere Datenbanken aufzubauen, die Daten unterschiedlicher Strafverfolgungs- und Geheimdienstbehörden zusammenführen sollen. Es ist davon auszugehen, dass all diese Datenbanken mit *data mining*-Techniken arbeiten (wollen). Im Januar 2003 hat George W. Bush z.B. die Einrichtung einer neuen Geheimdienstbehörde zur Terrorismusbekämpfung angekündigt. Im neu einzurichtenden *Terrorist Threat Integration Center* (TTIC) sollen FBI, CIA, *Homeland Security*-Ministerium und Verteidigungsministerium „merge and analyze all threat information in a single location" (Bush 2003). Das TTIC soll als Aufsichtsbehörde für nationale Anti-Terror-Projekte dienen, verteilte Datenbanken aufbauen und unterhalten und vollständigen Zugriff auf alle Informationen aller Geheimdienste haben. Es geht also auch beim TTIC weniger um traditionelle Überwachung oder Informationsgewinnung, sondern um Auswertung. Offensichtlich geht man von einer höheren öffentlichen Akzeptanz für die Auswertung von Informationen/Daten aus als für die Gewinnung neuer Daten und versucht das entsprechend zu vermitteln. Der Sprecher des *White House*, Ari Fleischer meinte z.B. in einem Presseinformationsgespräch zum TTIC am 29. Januar 2003:

> (TTIC) is an analytical unit. It is not a collection unit, which is something else I saw in one of the papers this morning, that reported that it would both collect and analyze. It would not collect. Collecting remains an area that other agencies do. The CIA does it. Interestingly, Homeland Security has the ability on its own to collect information, because, of course, they have Coast Guard as part of them, TSA as part of them, Secret Service as part of them (Fleischer 2003).

Das TTIC ist nicht zu verwechseln mit dem TSC, dem *Terrorist Screening Center*, einer Datenbank mit Namen von Terrorismusverdächtigen, die seit Dezember 2003 als zentrale Datenbank unter dem Dach des FBI existiert. Auch diese führt Informationen der unterschiedlichen Inlands- und Auslandsgeheimdienste zusammen, dient aber lediglich der vereinfachten zentralen Abfrage – so kann die *California Highway Patrol* routinemäßig im

Rahmen von Verkehrskontrollen überprüfen, ob es sich bei dem Verkehrssünder zufälligerweise um einen gesuchten Terroristen handelt. In der Datei befinden sich nach Angaben der Regierung die Daten von 120.000 Terrorismusverdächtigen, zur Herkunft dieser Daten gibt es keine rechte Antwort, auch nicht in dem Bericht der Leiterin des TSC – es macht aber stutzig, dass es dieselbe Anzahl von potentiellen TerroristInnen ist, die auch die Firma *Seisint* mit ihrem Terrorismus-Quotienten nach dem 11. September ermittelt hatte. Langfristig soll aber die Datenbank des TSC unter der Leitung des TTIC stehen und von dort gefüttert und gepflegt werden.

Anhand der hier erläuterten Beispiele sollte deutlich geworden sein, dass die US-Regierung auch zukünftig ihre Bestrebungen fortsetzen wird, große zentralisierte Datenbanken zu schaffen und *data mining* als zentrales Instrument der Terrorismusbekämpfung zu etablieren.

6. Ende oder Grenzen eines Abwehrrechtes?

In vielen Teilen der amerikanischen Gesellschaft, besonders unter Bürgerrechtlern und kritischen JuristInnen wird daher diskutiert, wie auf die neuen *Privacy*-Bedrohungen zu reagieren sei. Traditionell ist in den USA in Fragen informationeller Privatheit häufig eine Politik der Selbstregulierung vertreten worden (Westin 2003). In diesem Fall würde das heißen, dass sich der/die einzelne BürgerIn bemüht, weniger Daten zu produzieren, d.h. eine geringere Datenspur zu hinterlassen. Ein Ansatz, der sinnvoll, aber in vielerlei Hinsicht nicht praktikabel ist: Zum einen gibt es viele Verfahren, bei denen die Herausgabe von Daten in den USA zwingend erforderlich ist – zum Erhalt eines Führerscheins werden ein Photo und persönliche Informationen verlangt –, und zum anderen ist es wenig realistisch darauf zu bauen, dass Menschen auf Bequemlichkeiten wie z.B. bargeldlosen Geldtransfer oder Bezahlung verzichten. Ein weitere Möglichkeit wäre, Vorkehrungen zu treffen, dass entstandene Daten nicht weitergegeben werden. Der Aufwand, der hierfür betrieben werden muss, ist aber in Relation zum Privatheitsgehalt der Einzelinformation zumeist unverhältnismäßig hoch – und wird hoch gehalten.[17] Die dritte Möglichkeit wäre, dass der/die Einzelne versucht seine bzw. ihre Daten, da wo es technisch möglich ist, durch sogenannte *Privacy Enhancing Technologies* (v.a. unterschiedliche Verschlüsselungsprogramme) zu schützen. Zweifelhaft ist aber zum einen, wieviel Verschlüsselung der Staat bereit ist, seinen BürgerInnen rechtlich zuzugestehen, und zum anderen, ob das technische Wettrennen von Ver- und Entschlüsselung von den BürgerInnen gewonnen werden kann: „(T)he resulting surveillance arms race can hardly favor the ‚little guy'. The rich, the powerful, police agencies, and a technologically skilled elite will always have an advantage" (Brin zit. nach Froomkin 2000, 1539). Verschlüsselung kann sinnvoll sein, weil durch sie erst die „reasonable expectation of privacy" nach dem *Fourth Amendment* begründet wird, aber:

> The reasonable approach is not to invite an arms race by requiring that those who seek privacy employ the most recent, most sophisticated technologies to invoke the privilege of privacy. Predicating invocation on the sophistication of the countermeasures one employs is an unreasonable approach ..., it ultimately pits individual privacy against government technology, a battle the individual is destined to lose (Brenner 2002, 170).

Sich auf die Selbstregulierung der Wirtschaft zu verlassen, die doch von der Datenerhebung erheblich profitiert, erscheint illusorisch – solange nicht die Drohung der staatlichen Regulierung ernsthaft im Raum steht. Froomkin (2000, 1528) zitiert treffend Clarke: „Wolves self-regulate for the good of themselves and the pack, not the deer."

Ein weiterer Ansatz in den USA, mit der Datenflut und dem Verlust an Privatheit umzugehen, ist die Idee, dass diese Entwicklung zwar nicht revidierbar sei (die Büchse der Pandora lässt sich nicht schließen), sich aber zumindest die Ungleichheit in der Distribution von Informationen (und Macht) verringern ließe. Ein Instrument dabei ist der *Freedom of Information Act,* aber es gibt auch andere konkrete Projekte

in diesem Bereich, wie z.B. das Projekt *Government Information Awareness* am *Massachusetts Institute of Technology* in Boston, das feststellt: „In the United States, there is a widening gap between a citizen's ability to monitor his or her government and the government's ability to monitor a citizen." Das selbsterklärte Ziel ist: „To empower citizens by providing a single, comprehensive, easy-to-use repository of information on individuals, organizations, and corporations related to the government of the United States of America" (http://opengov.media.mit.edu/).

Auf die Rechtsprechung des *Supreme Court* in diesem Bereich zu hoffen, erscheint angesichts der bisherigen verfassungsrechtliche Beurteilung der von zentralisierten Datenbanken und *data mining* ausgehenden *Privacy*-Gefährdung wenig Erfolg versprechend. Wie mehrfach erwähnt, ist die vom *Fourth Amendment* geschützte *Privacy* lediglich ein Abwehrrecht gegen staatliche Eingriffe in die Privatsphäre:

> Whatever right to informational privacy may exist today, it is a right against governmentally sponsored invasions of privacy only – it does not reach private conduct. In addition, the government has unmatched power to centralize all the private sector data that is being generated. In fact, the distinction between government and private-sector privacy invasions is fading quickly. The Justice Department, for example, reportedly has an $8 million contract with data aggregator ChoicePoint that allows government agents to tap into the company's vast database of personal information on individuals (Stanley/Steinhardt 2003, 7f.).

Zum anderen handelt es sich bei den Daten, die in staatlichen und privatwirtschaftlichen Datenbanken zusammengeführt und analysiert werden, zumeist um Daten, die die BürgerInnen irgendwann einmal freiwillig an Dritte weitergegeben haben und die daher nach der Logik des *Supreme Court* nicht als privat zu werten und zu schützen sind.

Auch die zivilrechtliche Beschränkung von Datenaggregation und *data mining* nach Warren und Brandeis' ursprünglicher „*tort law privacy*" ist so nicht anwendbar, da hier eigentlich unwichtige Daten gespeichert und korreliert werden, also Informationen, die für sich genommen keinen vertraulichen Charakter haben. Der Informations*kontext* findet hierbei bisher keine Berücksichtigung. In der Literatur gibt es Versuche einer konzeptionellen Neufassung informationeller Privatheit, die diesen Kontext stärker berücksichtigt, nämlich die Tatsache, dass Information immer in einem spezifischen Zusammenhang steht, d.h. sie wird in der Regel einem/r bestimmten EmpfängerIn zu einem bestimmten Zweck gegeben. Die Speicherung, Proliferation und Rekombination der Information löst sie aus diesem ursprünglichen Zusammenhang und kann somit unabhängig vom Gehalt der Information eine *Privacy*-Verletzung darstellen (Nissenbaum 2004). Es bleibt abzuwarten, ob ein so verändertes *Privacy*-Konzept tatsächlich eine Chance darstellt, Warren und Brandeis' *Privacy* zu modernisieren.

Es scheint, als bedürften die USA, um den neuen Gefährdungen von Privatheit, die in Form von *data mining* auftreten, entgegenzutreten, eines veränderten rechtlichen Begriffs von *Privacy*, der über die bisherige verfassungs- und zivilrechtlichen Auffassungen von *Privacy* hinausgeht. Dieser müsste idealerweise die Form eines positiven Rechts auf Privatheit annehmen und verfassungsmäßig – in Form eines *Amendments* – verankert werden. Auf der Ebene der Landesverfassungen gibt es dies in den USA bereits in einigen Bundesstaaten. In Kalifornien z.B. heißt es in der Verfassung bereits seit 1972 im ersten Abschnitt des ersten Verfassungsartikels: „All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy" (http://www.leginfo.ca.gov/const.html). Es ist jedoch höchst unwahrscheinlich, dass es zu einer derartigen Regelung kommt, sowohl angesichts des derzeitigen politischen Klimas als auch angesichts verfassungsrechtlicher Bedenken. Da dies nicht zu erwarten ist, wären andere, kleinere Lösungen bereits ein großer Fortschritt, doch sind sie zur Zeit gleichermaßen unwahrscheinlich.

Wichtig wäre eine Gesetzgebung, die nicht länger zwischen privatwirtschaftlich und staatlich erhobenen Daten unterscheidet, mindestens

aber die konsequente Anwendung des *Privacy Act* von 1974 auf kommerzielle Datenbankenanbieter, wenn diese staatliche Aufgaben übernehmen. Der *Privacy Act* hatte sich auf staatliche Datensammlungen beschränkt, weil man davon ausging, lediglich der Staat habe die Ressourcen für große zentrale Datenbanken und nur der Staat könne ein Interesse daran haben solche aufzubauen. In welchem Maße der Staat auch Überwachungs- und Sicherheitsaufgaben „outsourcen" würde, nicht nur um Geld zu sparen, sondern auch um bestehende Begrenzungen staatlichen Handelns zu unterlaufen, scheint 1974 nicht vorstellbar gewesen zu sein. Aber wie schon Brandeis und Warren im ersten Satz ihres Aufsatzes (1890, 193) formulieren: „That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection." Ein solcher Zeitpunkt ist heute sicherlich gegeben.

ANMERKUNGEN

1 Den Begriff „*Privacy*" gibt es so im Deutschen nicht. Zwar ist letzthin versucht worden, mit „Privatheit" ein funktionales Äquivalent zu finden (z.B. Rössler 2001), es bleibt aber eine Hilfskonstruktion. Es wird im Deutschen eher vom Schutz der Privatsphäre gesprochen, worunter ein aus dem Recht auf freie Entfaltung der Persönlichkeit und auf Achtung der Menschenwürde abgeleitetes Recht auf einen unantastbaren Bereich des Lebens, aus dem die Öffentlichkeit ausgeschlossen ist, gemeint ist. Dazu gehören auch einzelne explizite Rechte wie das Brief- oder Fernmeldegeheimnis, die Unverletzlichkeit der Wohnung oder auch das Recht auf informationelle Selbstbestimmung, d.h. das Recht des/der Einzelnen, über die Preisgabe und Verwendung seiner/ihrer persönlichen Daten selbst zu bestimmen, soweit nicht stärkere Interessen des Allgemeinwohls dieses Recht einschränken.

2 Zusätzlich zu erwähnen wäre auch noch, dass es eine bestimmte Form von Privatheit gibt, die sich aus dem im *Fifth Amendment* festgelegten Privileg ableitet, sich nicht selber belasten zu müssen (Brenner 2002).

3 Rössler beschäftigt sich länger mit der Frage, warum jemand, der unter Beobachtung steht, in seiner Freiheit eingeschränkt ist, obwohl er immer noch tun und lassen kann, was er will. Sie treibt die Fragestellung auf die Spitze, indem sie behauptet, dass auch derjenige, der keine Kenntnis davon hat überwacht zu werden, nicht mehr in der Lage sei, autonom zu sein, weil nämlich sein Denken und Handeln auf einer falschen Voraussetzung beruhe – nämlich der unbeobachtet zu sein. Eine signifikante Verletzung informationeller Privatheit ist nach Rössler (2001, 207f.) auch dann gegeben, „wenn eine Person ... nie davon erfährt, dass sie beobachtet oder gefilmt wurde: denn ihr Verhalten war ein Verhalten ‚unter falschen Bedingungen'."

4 Eine gute Einführung in die Tradition des *Privacy*-Konzeptes im amerikanischen Recht bietet Gormley (1992). Ansonsten hat sich Westin bereits 1967 in seinem Standardwerk mit der historischen Kontextualisierung von *Privacy*-Konzepten in der amerikanischen Rechtstradition beschäftigt.

5 Vielleicht entbehrt es nicht einer gewissen Ironie, dass *Privacy* als Rechtsbegriff seinen Ursprung im Privatrecht hat, obwohl später *Privacy* überwiegend als Abwehrrecht gegen staatliche Verletzungen der Privatsphäre begriffen wurde.

6 Genauer hierzu Brenner 2002.

7 Es sind trotz aller negativen Entwicklungen auch kleine Anzeichen einer Erholung in diesem Bereich feststellbar: in Kalifornien z.B. ist im Sommer 2004 eines der umfassendsten *Online Privacy*-Gesetze verabschiedet worden.

8 Auf den problematischen Entstehungszusammenhang des *USA PATRIOT Act* bin ich an anderer Stelle ausführlicher eingegangen (Rürup 2002; 2003; 2004).

9 Eine andere Bezeichnung für *National Security Letters* ist „*admistrative subpoenas*" – diese Bezeichnung macht deutlicher, um was es sich eigentlich handelt: die Herausgabe von Dokumenten verlangt mit Strafandrohung auf dem Verwaltungsweg.

10 Entgegen den Äußerungen von George W. Bush im Wahlkampf gehört Section 505 nicht zu den Teilen des *PATRIOT Act*, die automatisch auslaufen. Seine Äußerungen hierzu sind aber charakteristisch für die Darstellung der Sicherheitspolitik durch die amtierende Regierung: „By the way, the reason I bring up the Patriot Act, it's set to expire next year. I'm starting a campaign to make it clear to members of Congress it shouldn't expire. It shouldn't expire, for the security of our country. (Applause.) Administrative subpoenas mean, it is – speeds up the process whereby people can gain information to go after terrorists. Administrative subpoenas I guess is kind of an ominous sounding word, but it is, to put everybody's mind at ease about administrative subpoenas – we use them to catch crooked doctors today. It's a tool for people to chase down medical fraud. And it certainly makes sense to me that if we're using it as a tool to chase medical fraud cases, we certainly ought to use it as a tool to chase potential terrorists" (Bush 2004).

11 Zu den National Security Letters gibt es noch eine (zum Zeitpunkt der Fertigstellung dieses Beitrags brandaktuelle) Neuigkeit: In Manhattan hat am 29. September 2004 der Richter Victor Marrero die Praxis, mit *National Security Letters* Internetprovider

zur Herausgabe ihrer Kundendaten zu zwingen, für rechtlich unzulässig erklärt (http://www.watchingjustice.org/whatsnew/whatsnew.php?docId=446).

12 Im Entwurf des *PATRIOT II Act* war die Möglichkeit der Ausbürgerung von US-Staatsbürgern vorgesehen. Nach Abschnitt 501 wäre es möglich gewesen, US-Bürgern aufgrund der Mitgliedschaft in oder Unterstützung von terroristischen Vereinigungen ihre Staatangehörigkeit abzuerkennen (vgl. Cole 2003a, b).

13 Für nähere Informationen zu *ChoicePoint* und anderen kommerziellen Datenanbietern vgl. Hoofnagel 2004, 600.

14 Das Vertrauen in die Vertraulichkeit gerade der von der Zensus erhobenen Daten ist zur Zeit jedoch erschüttert. Im Sommer 2004 gab das Zensusbüro an *Homeland Security* im Zuge der Amtshilfe Daten von EinwohnerInnen weiter, die sich selbst beim Zensus als arabischer Herkunft identifiziert hatten. Zu den Informationen gehörte u.a. die Angabe von Gemeinden, in denen mehr als 1000 AmerikanerInnen arabischer Herkunft ansässig seien (Clemetson 2004).

15 Ein besonders im internationalen Kontext interessanter Aspekt ist die Tatsache, dass die kommerziellen Datenbankanbieter auch Daten in anderen Ländern einkaufen (z.B. Mexiko, Costa Rica und Nicaragua) und diese amerikanischen Behörden wie dem *Immigration and Naturalization Service* anbieten.

16 Auf einen weiteren wichtigen Problembereich kann hier leider nicht eingegangen werden, nämlich die langfristige Verwendung solcher Methoden zur sozialen Klassifizierung, Überwachung, Ausgrenzung und Kontrolle (Lyon 2001; 2002a; 2002b).

17 Froomkin (2000, 1502) konstatiert, die KonsumentInnen litten an „*privacy myopia*“: „(T)hey will sell their data too often and too cheaply.“ Er erklärt diese Kurzsichtigkeit damit, dass die Gesamtheit der in einem Profil gesammelten Daten an Wert die Summe der dort zusammengeführten Einzeldaten weit übersteigt. Der/die einzelne KonsumentIn wird den Wert der Daten, die er/sie bei einer Transaktion „verkauft“, an dem Maß an Privatheit bemessen, das er/sie damit aufgibt. Für den Käufer bzw. Wiederverkäufer bemisst sich der Wert an dem daraus entstehenden Profil. Die Datenakkumulation steigert den Wert der Daten so, wie das Maß an Privatheitsverlust die Summe der Einzelinformationen übersteigt.

LITERATUR

ACLU (American Civil Liberties Union) (2004a). Documents Acquired By ACLU Prove That MATRIX is a Data Mining Program, January 21, 2004. Internet: http://www.aclu.org/Privacy/Privacy.cfm?ID=14763&c=130.

ACLU (American Civil Liberties Union) (2004b). GAO Report Reveals Four Potential Government Data-Surveillance Programs, ACLU Says, May 27, 2004. Internet: http://www.aclu.org/Privacy/Privacy.cfm?ID=15860&c=130.

Arzt, Clemens (2004). Polizeiliche Überwachungsmaßnahmen in den USA. Grundrechtsbeschränkungen durch moderne Überwachungstechniken und der War on Terrorism, Frankfurt am Main.

Brenner, Susan W. (2002). The Privacy Privilege: Law Enforcement, Technology, and the Constitution, in: University of Florida Journal of Technology Law & Policy, 7(2), 123–194.

Bush, George W. (2003). State of the Union Address, 28. Januar 2003, The U.S. Capitol. Internet: http://www.whitehouse.gov/news/releases/2003/01/20030128-19.html.

Bush, George W. (2004). Information Sharing, Patriot Act Vital to Homeland Security. Rede des Präsidenten am 20. April 2004 in Buffalo, New York. Internet: http://www.whitehouse.gov/news/releases/2004/04/20040420-2.html.

Cate, Fred H. (2001). Privacy and Other Civil Liberties in the United States after September 11, American Institute for Contemporary German Studies, The Johns Hopkins University, 1–19. Internet: http://www.aicgs.org/Publications/PDF/cate.pdf.

Chang, Nancy (2001). The USA PATRIOT Act: What's So Patriotic About Trampling on the Bill of Rights?, Center for Constitutional Rights. Internet: http://www.ratical.org/ratville/CAH/USAPAanalyze.pdf.

Clarke, Roger (1988). Information Technology and Dataveillance, in: Communications of the ACM 31(5), 498–512. Internet: http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html.

Clarke, Roger (1997). Privacy and Dataveillance, and Organisational Strategy. Internet: http://www.anu.edu.au/people/Roger.Clarke/DV/PStrat.html.

Clemetson, Lynette (2004). Homeland Security Given Data on Arab-Americans, in: New York Times, 30. Juli 2004, Section A, Spalte 1, 14.

Cole, David (2003a). Operation Enduring Liberty, in: The Nation. Internet: http://www.thenation.com/doc.mhtml%3Fi=20020603&s=cole.

Cole, David (2003b). What Patriot II Proposes to Do, Center for Democracy and Technology. Internet: http://www.cdt.org/security/usapatriot/030210cole.pdf.

DARPA (Defense Advanced Research Projects Agency) (2003). Report to Congress regarding the Terrorism Information Awareness Program. In response to Consolidated Appropriations Resolution, 2003, Pub. L. No. 108–7, Division M, § 111(b). Executive Summary. Internet: http://www.globalsecurity.org/security/library/report/2003/tia-exec-summ_20may2003.pdf.

Dempsey, James/Lara *Flint* (2004). Privacy's gap: The Largely Non-Existent Legal Framework for Government Mining of Commercial Data, Center for Democracy and Technology. Internet: http://www.cdt.org/security/usapatriot/030528cdt.pdf.

Fleischer, Ari (2003). Pressebriefing an Bord der Air Force One auf dem Weg nach Grand Rapids, Michigan, 29. Januar 2003. Internet: http://www.whitehouse.gov/news/releases/2003/01/20030129-6.html#6.

France, Mike/Heather *Green* (2001). Privacy in an Age of Terror, in: Business Week, 5. November 2001, 82.

Froomkin, A. Michael (2000). The Death of Privacy?, in: Stanford Law Review, 52, 1461–1543. Internet: http://www.law.miami.edu/~froomkin/articles/privacy-deathof.pdf.

GAO (United States General Accounting Office) (2004). Report to the Ranking Minority Member, Subcommittee on Financial Management, the Budget, and International Security, Committee on Governmental Affairs, U.S. Senate: DATA MINING Federal Efforts Cover a Wide Range of Uses. Internet: http://www.gao.gov/new.items/d04548.pdf.

Gormley, Ken (1992). One Hundred Years of Privacy, in: Wisconsin Law Review. Internet: http://cyber.law.harvard.edu/privacy/Gormley—100%20Years%20of%20Privacy.htm.

Hoofnagle, Chris Jay (2004). Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement, in: North Carolina Journal of International Law & Commercial Regulation, 29(4), 595–636.

Lepsius, Oliver (2002). Das Verhältnis von Sicherheit und Freiheitsrechten in der Bundesrepublik Deutschland nach dem 11. September 2001, American Institute for Contemporary German Studies, The Johns Hopkins University, 1–26. Internet: http://webdoc.sub.gwdg.de/ebook/lf/2003/aicgs/publications/PDF/lepsius.pdf.

Lyon, David (2001). Surveillance after September 11, in: Sociological Research Online, 6(3). Internet: http://www.socresonline.org.uk/6/3/lyon.html.

Lyon, David (2002a). Surveillance as Social Sorting. Privacy, Risk and Digital Discrimination, London/New York.

Lyon, David (2002b). Surveillance Studies: understanding visibility, mobility and the phenetic fix, in: Surveillance & Society, 1(1), 1–7. Internet: http://www.surveillance-and-society.org/articles1/editorial.pdf.

Nissenbaum, Helen (2004). Privacy as Contextual Integrity, in: Washington Law Review, 79(1), 119–158. Internet: http://www.law.washington.edu/WLR/nissenbaum.pdf.

o.A. (2003). JetBlue Airways Gave Defense Dept Itineraries of 5 Million Customers Airline Passengers' Data Used in Study Published on Saturday, in: Oakland Tribune, 20. September 2003. Internet: http://commondreams.org/headlines03/0920-01.htm.

Ramasastry, Anita (2002). Why We Should Be Concerned about „Total Information Awareness" and Other Anti-Terrorism Strategies for the Internet. Internet: http://writ.corporate.findlaw.com/ramasastry/20021231.html.

Regan, Priscilla M. (2003). Safe Harbors or Free Frontiers? Privacy and Transborder Data Flows, in: Journal of Social Issues, 59(2), 263–282.

Rössler, Beate (2001). Der Wert des Privaten, Frankfurt am Main.

Rötzer, Florian (2003). Matrix ist in Florida, in: Telepolis. Magazin der Netzkultur, 6. August 2003. Internet: http://www.heise.de/tp/deutsch/inhalt/te/15388/1.html.

Rürup, Katharina Sophie (2002). Bürgerrechte Adé? Die Gesetzgebung in den USA nach dem 11. September, in: vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftspolitik, 41(3), 52–60.

Rürup, Katharina Sophie (2003). Sicherheit ohne Freiheit, in: Ansprüche. Forum demokratischer Juristen und Juristinnen, 11(1), 24–29.

Rürup, Katharina Sophie (2004). Die bedrohte Freiheit. Eine Neuerscheinung zur amerikanischen Grundrechtspraxis, in: vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftspolitik, 43(3), 109–111.

Stalder, Felix (2002). Opinion: Privacy is not the antidote to surveillance, in: Surveillance & Society 1(1), 120–124. Internet: http://www.surveillance-and-society.org/articles1/opinion.pdf.

Stanley, Jay/Barry *Steinhardt* (2003). Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society, American Civil Liberties Union (ACLU), New York. Internet: http://www.aclu.org/Files/OpenFile.cfm?id=11572.

Stratford, Jean Slemmons/Juri *Stratford* (1998). Data Protection and Privacy in the United States and Europe, Paper präsentiert bei der IASSIST-Konferenz, 21. Mai 1998. Internet: http://iassistdata.org/publications/iq/iq22/iqvol223stratford.pdf.

Warren, Samuel D./Louis D. *Brandeis* (1890). The Right to Privacy, in: Harvard Law Review, 4, 193–220. Internet: http://www.louisville.edu/library/law/brandeis/privacy.html.

Westin, Alan F. (1967). Privacy and Freedom, New York.

Westin, Alan F. (2003). Social and Political Dimensions of Privacy, in: Journal of Social Issues, 59(2), 431–453.

URTEILE DES SUPREME COURT

California v. Ciraolo, 476 U.S. 207 (1986). Internet: http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=476&invol=207.

Katz v. United States, 389 U.S. 347 (1967). Internet: http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=389&invol=347.

Kyllo v. United States, 533 U.S. 27 (2001). Internet: http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=533&invol=27.

Olmstead v. United States, 277 U.S. 438 (1928). Internet: http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=us&vol=277&invol=438.

United States v. Miller, 425 US 435 (1976). Internet: http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=425&invol=435.
U.S. Supreme Court Roe v. Wade, 410 U.S. 113 (1973). Internet: http://caselaw.lp.findlaw.com/scripts/etcase.pl?court=US&vol=410&invol=113.

GESETZE

Computer Security Act of 1987 (1987). Pub. L. 100–235 (HR 145).
Computer Matching and Privacy Protection Act (CMPPA) (2000). 5 U.S.C. § 552a (2000).
Department of Defense Appropriations Act, H.R.2658 „*Limitation on use of funds for research and development on Total Information Awareness Program*" (2004). Internet: http://thomas.loc.gov/cgi-bin/bdquery/z?d108:h.j.res.00002.
Domestic Security Enhancement Act 2003 (Draft) (USA PATRIOT Act II) (2003). Internet: http://www.publicintegrity.org/dtaweb/downloads/Story_01_020703_Doc_1.pdf.
Electronic Communications Privacy Act of 1986 (1986). Pub. L. No. 99–508, 100 Stat. 1848 (1986).
FISA – Foreign Intelligence Surveillance Act of 1978 (1978). Pub. L. No. 95– 511. Internet: http://www4.law.cornell.edu/uscode/50/ch36.html.
Freedom of Information Act, 5 U.S.C. § 552 (1966).
Haushalt 2004, Section 8124. Limitation on Deployment of Terrorism Information Awareness Program (2004).
National Education Statistics Act of 1994 (1994).
Right to Financial Privacy Act (2000). 12 U.S.C. §§ 3401–3422 (2000).
Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act (2001). Pub. L. No. 107–56, 115 Stat. 272. Internet: http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3162.ENR.

AUTORIN

Katharina Sophie RÜRUP. Studium der Amerikanistik und Politikwissenschaft an der FU Berlin; Mitarbeit in einem Forschungsprojekt zu nationaler Identität und Staatsbürgerschaft in den USA an der TU-Dresden; lange Zeit Mitglied im Berliner Landesvorstand der Humanistischen Union. Beschäftigt in der politischen Bildungsarbeit und als wissenschaftliche Übersetzerin. Forschungsschwerpunkte: amerikanische Innenpolitik, Geschichte der Bürgerrechtsbewegungen in den USA und die Rechtssprechung des Supreme Courts.

E-mail: ksrueru@zedat.fu-berlin.de